UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF TEXAS

REINALDO AGUIAR, individually and on behalf of all others similarly situated,

Plaintiff,

ELON MUSK, an individual residing in California and Texas;

TRAVIS KALANICK, an individual residing in New York, NY and Los Angeles, CA;

DAVID F. HINE, an attorney residing in Ohio and Partner at the Law Firm Vorys, Sater, Seymour and Pease LLP;

JAMES CASEY, an individual residing in the United States, believed to be a collaborator in cyber-attacks against competitors of the Defendants;

WILMER RUPERTI, an individual residing in Florida and New York believed to be involved in the relevant operations managed by the Defendants;

and

JOHN DOES 1-100, unknown individuals and entities who participated in the conduct alleged herein,

Defendants.

CLASS ACTION COMPLAINT

Plaintiff Reinaldo Aguiar ("Plaintiff"), individually and on behalf of all persons similarly situated, alleges the following against Defendants:

NATURE OF THE ACTION

1. Plaintiff Reinaldo Aguiar, proceeding *pro se* and on behalf of all others similarly situated (the "Class"), brings this class action for violations of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2511, *et seq.*, and related state laws.
2. This action arises from Defendants' alleged unlawful interception, access, and monitoring of the electronic communications and private whereabouts of technology company employees, including Plaintiff and Class Members, without their consent.

THE PARTIES

3. Plaintiff Reinaldo Aguiar is an adult individual residing in Fort Bend County, Texas.
4. Upon information and belief, Plaintiff Aguiar was employed by various technology company teams, allegedly under the direct or indirect control or influence of one or more Defendants, for approximately eighteen (18) years, from on or around 2005 through 2023. These companies include Merlin Edge Inc. (2005), Shaw Communications (2007-2009), Yahoo!

Inc. (2009-2010), Google LLC (2010-2018), Goldman Sachs LLC (2018-2020), and Twitter Inc./X Corp. (2020-2023).

5. Upon information and belief, Defendant Elon Musk is an individual residing in California and Texas, with significant control and influence over various technology companies, including X Corp. (formerly Twitter Inc.) and Tesla, Inc.
6. Upon information and belief, Defendant Travis Kalanick is an individual residing in New York, NY, and Los Angeles, CA, and is a co-founder of Uber Technologies, Inc.
7. Upon information and belief, Defendant David F. Hine is an attorney-at-law, licensed in Ohio, and a Partner at the law firm Vorys, Sater, Seymour and Pease LLP.
8. Upon information and belief, Defendant James Casey is an individual residing in the United States, believed to be a collaborator in cyber-attacks against competitors of the Defendants.
9. Upon information and belief, Defendant Wilmer Ruperti is an individual residing in Florida and New York, believed to be involved in the relevant operations managed by the Defendants.
10. Upon information and belief, Defendants, acting individually and in concert, as well as through separate and seemingly disconnected entities, engaged in a pattern of unlawful conduct as further described herein.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over Plaintiff's and the Class's federal law claims pursuant to 28 U.S.C. § 1331 (federal question jurisdiction) as this action arises

under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511 *et seq*.

12. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367, as those claims are so related to the federal claims that they form part of the same case or controversy.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in this District, Defendants conduct substantial business in this District, and/or Plaintiff resided and worked in this District for companies allegedly controlled or influenced by Defendants at the time of the alleged unlawful conduct.

14. Venue is also proper in this District because, upon information and belief, Defendants received, managed, accessed, intercepted, and transmitted communications collected from individuals, including Plaintiff, within this District.

15. In connection with the acts complained of herein, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including the internet.

CLASS ACTION ALLEGATIONS

16. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and all other persons similarly situated. Plaintiff seeks to represent the following classes:

    - **The National Class:** All individuals in the United States who (1) worked as engineers or engineering managers for

companies directly or indirectly controlled or influenced by one or more of the Defendants, and (2) whose private electronic communications and/or location data were unlawfully intercepted, accessed, and/or monitored by or at the direction of Defendants without their consent.

- **The Texas Wiretap Law Subclass:** All individuals in Texas who (1) worked as engineers or engineering managers for companies directly or indirectly controlled or influenced by one or more of the Defendants, and (2) whose private electronic communications and/or location data were unlawfully intercepted, accessed, and/or monitored by or at the direction of Defendants without their consent (the "Texas Subclass").

17. The "Class Period" dates back four years (or the length of the longest applicable statute of limitations for any claim asserted) from the filing of this Complaint and continues through the date of judgment.

18. Excluded from the Classes are: (a) any officers and directors of companies controlled by the Defendants during the Class Period involved in directing the alleged unlawful conduct; (b) any judge assigned to hear this case (or spouse or family member of any assigned judge); (c) any employee of the Court; and (d) any juror selected to hear this case. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

19. **Numerosity (Fed. R. Civ. P. 23(a)(1)):** The proposed Classes are so numerous that joinder of all members would be

impracticable. Upon information and belief, technology companies associated with or influenced by Defendants employ tens of thousands, if not hundreds of thousands, of engineers. Even a fraction of these individuals being targeted would result in thousands of Class Members. Plaintiff estimates the National Class may number 25,000 individuals or more, with at least 1,000 such individuals residing in Texas.

20. **Commonality (Fed. R. Civ. P. 23(a)(2))**: There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual members. Common questions include, but are not limited to:

- Whether Defendants engaged in the unauthorized interception of electronic communications of Plaintiff and Class Members;
- Whether Defendants utilized a system (referred to by Plaintiff as the "UBER of Espionage" geo-index and associated tools) to track the locations of Plaintiff and Class Members;
- Whether Defendants procured others to intercept such communications or track such locations;
- Whether Defendants' conduct violated the ECPA;
- Whether Defendants' conduct violated the Texas Wiretap Law (for the Texas Subclass);
- Whether Defendants' conduct constituted an invasion of privacy;
- The nature and extent of injunctive relief appropriate to remedy Defendants' conduct; and

- The appropriate measure of damages.

21. **Typicality (Fed. R. Civ. P. 23(a)(3)):** Plaintiff's claims are typical of the claims of the Class Members. Plaintiff, like all Class Members, was allegedly injured by Defendants' unauthorized interception, collection, and/or monitoring of his personal electronic communications and location data through a common scheme.

22. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)):** Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has no interests antagonistic to those of other Class Members. Plaintiff has personally observed, documented, and analyzed the alleged surveillance operations forming the basis of this Complaint. Plaintiff intends to retain appropriate legal counsel prior to trial to assist in the prosecution of this class action.

23. **Predominance and Superiority (Fed. R. Civ. P. 23(b)(3)):** Common questions of law and fact predominate over any questions affecting only individual Class Members. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Given the alleged secretive nature of Defendants' conduct and the potential expense of individual litigation, it would be impracticable for most Class Members to seek individual redress.

    - Individual Class Members may be unaware they have been wronged due to the clandestine nature of the alleged surveillance.
    - Concentration of this litigation in one forum is desirable.

- The difficulties likely to be encountered in the management of this class action are not insurmountable.

24. **Injunctive Relief (Fed. R. Civ. P. 23(b)(2)):** This action is also appropriate for certification under Rule 23(b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Classes, making appropriate final injunctive relief or corresponding declaratory relief with respect to the Classes as a whole. In the absence of injunctive relief, Class Members will continue to suffer irreparable harm.

SUBSTANTIVE ALLEGATIONS

25. Upon information and belief, Defendants, acting in concert and through various instrumentalities, have for many years operated and utilized a sophisticated, clandestine system for the unlawful wiretapping, surveillance, and monitoring of individuals, including Plaintiff and members of the Class.

26. This system involves, among other things, a vast geo-location database (referred to by Plaintiff as the "geo-index" or part of the "UBER of Espionage" platform) that contains or contained billions of specific geographical locations worldwide.

27. Upon information and belief, Plaintiff discovered the existence of this geo-index and, through technical analysis, determined that it was used to coordinate the tracking and interception of targeted individuals.

- Plaintiff alleges he located and downloaded a file containing this geo-index from a server on or around September 11, 2024.

- Plaintiff further alleges that the geo-index uses "encoders" to store location data in an obscured format.
- Between September and November 2024, Plaintiff developed a proprietary system to decode and analyze this geo-index, correlating its data with public records and other information to identify patterns and significant locations allegedly used by Defendants' network.

28. Upon information and belief, this geo-index allegedly contains "markers" or metadata indicating the importance or nature of specific locations, including locations Plaintiff believes are associated with "intelligence positions" and "military positions" used by Defendants' network.

29. Upon information and belief, data from this geo-index, as analyzed by Plaintiff's system, allegedly shows high concentrations of "scores" (a metric Plaintiff developed to rank location importance within the index) associated with properties and facilities linked to Defendant Elon Musk (e.g., Tesla Giga Factories in Austin, TX, and Berlin, Germany) and geographic locations allegedly used for routing communications (e.g., Venezuela, Texas).

30. Upon information and belief, between approximately 2014 and the present, Defendants used this geo-location database and associated technologies to:

- Track the physical whereabouts of Plaintiff and Class Members.
- Facilitate the physical interception of Plaintiff and Class Members by agents of Defendants for surveillance purposes.

- Intercept network traffic and electronic communications of Plaintiff and Class Members.
- Integrate with public online platforms like Google Maps and Google Street View, to use said platforms as means of covert communication and covert record-keeping related to their surveillance operations.
- Operate a covert communications network to transmit digital information locally and internationally in furtherance of their surveillance scheme.

31. Plaintiff alleges, based on his personal observations and analysis using his proprietary system, the following specific instances of surveillance targeting him and locations related to him, which he believes are part of Defendants' broader unlawful operations:
    - On or around January 27, 2025, Plaintiff conducted and recorded a technical demonstration (referenced in Plaintiff's Affidavit, attached hereto as Exhibit A) explaining the functionality of the geo-location database and its alleged use by Defendants.
    - On August 9, 2024, an individual driving a white truck followed Plaintiff and, upon Plaintiff entering the parking lot of Clear Channel Outdoors located at 12852 Westheimer Rd, Houston, TX 77077, this individual activated the automatic gates to trap Plaintiff on the premises.
    - On or around August 11, 2024, Plaintiff transmitted electronic correspondence to Phillip Edward Denning, in his capacity as President of the Lake Pointe Estates

Homeowners Association ("the Association"). Said correspondence notified Mr. Denning of the presence of alleged military-grade antennas on various properties within the Subdivision, without reference to any specific property address. In response, Mr. Denning asserted that such antennas were approved in accordance with Federal Communications Commission ("FCC") regulations. Subsequent to this exchange, and within approximately twenty-four (24) hours, an antenna consistent with the description of an "alleged military-grade antenna," which had been installed in the backyard of the property located at 24927, North Point Pl, Katy, Texas, was removed.

- On August 18, 2024, an individual at a park in Katy, TX, was observed recording and transmitting Plaintiff's location as Plaintiff passed nearby.
- On or around August 26, 2024, Plaintiff's system identified an 8-digit prefix match between the phone number of Francisco Castillo, a long-time friend of Plaintiff, and the phone number of Plaintiff's then-current landscaper, a statistical anomaly Plaintiff believes is indicative of surveillance coordination.
- On or around August 2024, Plaintiff's system detected that properties registered to Olesya Luzinova, a former close friend of Plaintiff, were being tracked by the aforementioned geo-location database.
- On or around January 10, 2025, Plaintiff's system discovered that the residence of Patricia Rojas, a long-

time family friend of Plaintiff, was being tracked by the geo-location database.

- On or around March 1, 2025, an individual, believed to be an agent of Defendants, emerged from a neighboring property at 24927 North Point Pl, Katy, TX, and attempted to intercept Plaintiff near his vehicle. When Plaintiff paused to avoid the interception, the individual turned and made a second attempt to intercept Plaintiff.
- On or around March 2025, Plaintiff's system identified that the residence located at 8926 Valley Side Dr, Houston, TX 77078, belonging to Marythe Oropeza (a former employee of Plaintiff who cared for Plaintiff's son), was being tracked by the geo-location database.
- On or around March 2025, Plaintiff's system discovered that the residence at 8918 Valley Side Dr, Houston, TX 77078, owned by Jose Castillo (a friend and former employee of Plaintiff), was being tracked by the geo-location database.
- On or around March 2025, Plaintiff's system discovered that the residence of Veronica Sanchez, CPA (Plaintiff's accountant for tax year 2022), was being tracked by the geo-location database.
- On March 5, 2024, Plaintiff met with an FBI agent at Campesino Coffee House, 2602 Waugh Dr, Houston, TX 77006, to report Defendants' alleged activities.

- On or around February 7, 2025, Plaintiff's system discovered that the address of Campesino Coffee House was being tracked by the geo-location database.
- On or around January 27, 2025, Plaintiff's system detected that all companies known to be owned or directed by Defendant Elon Musk were being tracked by the geo-location database.
- On at least two occasions between September 18, 2024, and May 4, 2025, a black Suburban SUV with vanity license plates "BRITOS 1" intercepted Plaintiff. In December 2024, the driver of this "BRITOS 1" SUV drove aggressively towards Plaintiff's vehicle, nearly causing a collision. On May 4, 2025, the "BRITOS 1" SUV was observed passing in front of Plaintiff's residence at 2302 Britton Ridge Drive, Katy, TX 77494.
- On or around February 11, 2025, Plaintiff's system discovered that Cinco Meadows Dental, located at 25900 Cinco Ranch Boulevard, Katy, TX 77494, where Plaintiff is a patient, was being tracked by the geo-location database.

32. Upon information and belief, Defendants and/or their agents purchased, leased, or otherwise utilized real estate properties neighboring the residences of Plaintiff and Class Members to install electronic equipment for visual and electronic surveillance and to intercept, decrypt, and gain unauthorized access to electronic communications, computer/network traffic, and trade secrets.

33. Upon information and belief, Defendants and/or their agents unlawfully gained access to private and confidential

information of Plaintiff and Class Members, including but not limited to medical records, insurance records, banking information, and securities transactions, potentially in violation of statutes such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA).

34. On or around September 2024, Plaintiff filed a complaint with the Office of the Attorney General of Texas, alleging illegal surveillance and wiretapping by parties including Defendant Travis Kalanick and others.

35. As of the date of this filing, Plaintiff has not received a substantive response from the Office of the Attorney General of Texas regarding that complaint.

36. The collective actions of the Defendants, as described herein, constituted a continuous pattern of unlawful surveillance and invasion of privacy against Plaintiff and the Class members, causing them significant harm.

CAUSES OF ACTION

COUNT I Violation of the Electronic Communications Privacy Act (ECPA) (18 U.S.C. § 2511) (On behalf of Plaintiff and the National Class)

37. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

38. Defendants intentionally intercepted, endeavored to intercept, and/or procured other persons to intercept or endeavor to intercept Plaintiff's and Class Members' electronic communications without their knowledge,

authorization, or consent, in violation of 18 U.S.C. § 2511(1)(a).

39. "Electronic communication" is defined in 18 U.S.C. § 2510(12) as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. Plaintiff's and Class Members' communications fall within this definition.

40. Defendants intentionally used, endeavored to use, and/or procured other persons to use or endeavor to use an electronic, mechanical, or other device to intercept Plaintiff's and Class Members' electronic communications, in violation of 18 U.S.C. § 2511(1)(b).

41. Defendants intentionally disclosed, endeavored to disclose, and/or procured other persons to disclose or endeavor to disclose to any other person the contents of Plaintiff's and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the unlawful interception of such communications, in violation of 18 U.S.C. § 2511(1)(c).

42. Defendants intentionally used, endeavored to use, and/or procured other persons to use or endeavor to use the contents of Plaintiff's and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the unlawful interception of such communications, in violation of 18 U.S.C. § 2511(1)(d).

43. Neither Plaintiff nor Class Members authorized or consented to Defendants' interception, disclosure, or use of their electronic communications.

44. As a direct and proximate result of Defendants' violations of the ECPA, Plaintiff and Class Members have suffered injury, including invasion of their privacy, and are entitled to relief pursuant to 18 U.S.C. § 2520, including declaratory relief, equitable relief, statutory damages of the greater of $10,000 per violation or $100 per day for each day of violation, actual damages, punitive damages, and reasonable attorneys' fees and costs.

COUNT II Violation of the Texas Wiretap Law (Tex. Code Crim. Proc. art. 18A.002) (On behalf of Plaintiff and the Texas Subclass)

45. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

46. The Texas Interception of Communications Act, Tex. Code Crim. Proc. art. 18A.002(a)(1), prohibits a person from intentionally intercepting, endeavoring to intercept, or procuring another person to intercept or endeavor to intercept a wire, oral, or electronic communication.

47. Defendants violated this provision by intentionally intercepting, endeavoring to intercept, or procuring others to intercept the electronic communications of Plaintiff and Texas Subclass Members in Texas without their consent.

48. Tex. Code Crim. Proc. art. 18A.002(a)(3) prohibits intentionally disclosing or endeavoring to disclose to another person the contents of a wire, oral, or electronic communication knowing or having reason to know that the information was obtained through unlawful interception.
49. Defendants violated this provision by intentionally disclosing or endeavoring to disclose the contents of unlawfully intercepted communications of Plaintiff and Texas Subclass Members.
50. Tex. Code Crim. Proc. art. 18A.002(a)(4) prohibits intentionally using or endeavoring to use the contents of a wire, oral, or electronic communication knowing or having reason to know that the information was obtained through unlawful interception.
51. Defendants violated this provision by intentionally using or endeavoring to use the contents of unlawfully intercepted communications of Plaintiff and Texas Subclass Members.
52. Neither Plaintiff nor Texas Subclass Members authorized or consented to Defendants' interception, disclosure, or use of their communications.
53. Pursuant to Tex. Civ. Prac. & Rem. Code § 123.004, Plaintiff and Texas Subclass Members are entitled to injunctive relief, actual damages, statutory damages of $10,000 for each occurrence, punitive damages, and attorney's fees and costs.

COUNT III Invasion of Privacy (Intrusion Upon Seclusion) (On behalf of Plaintiff and the National Class / or applicable State Subclasses)

54. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

55. Plaintiff and Class Members had a reasonable expectation of privacy in their private electronic communications, personal data, and physical whereabouts.

56. Defendants, through the conduct described herein, intentionally intruded upon the solitude, seclusion, and private affairs of Plaintiff and Class Members. This intrusion included, but was not limited to, the unauthorized interception of their electronic communications, surveillance of their physical locations, and access to their private data using means such as the "UBER of Espionage" geo-index, alleged spyware, and hardware interception devices.

57. Defendants' intrusion would be highly offensive to a reasonable person. The alleged surveillance was pervasive, clandestine, and targeted sensitive personal and professional information over an extended period.

58. As a direct and proximate result of Defendants' invasion of their privacy, Plaintiff and Class Members have suffered injury, including emotional distress, annoyance, and interference with their personal and professional lives.

59. Defendants' conduct was willful, wanton, and malicious, justifying an award of punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Classes, respectfully requests that this Court enter judgment against Defendants, jointly and severally, and grant the following relief:

A. Certifying this action as a class action pursuant to Fed. R. Civ. P. 23, appointing Plaintiff as Class Representative, and appointing appropriate Class Counsel;

B. For a Temporary Restraining Order and Preliminary and Permanent Injunctions enjoining Defendants, their officers, agents, servants, employees, and all persons in active concert or participation with them, from:

   i. Intercepting, accessing, monitoring, or disclosing the electronic communications or location data of Plaintiff and Class Members;

   ii. Physically approaching or conducting surveillance on Plaintiff and Class Members, their residences, places of business, or employment in furtherance of the unlawful activities alleged herein;

   iii. Utilizing the "UBER of Espionage" geo-index or any similar system for unlawful surveillance or interception;

C. For an order declaring that Defendants' acts and practices violate the ECPA;

D. For an order declaring that Defendants' acts and practices violate the Texas Wiretap Law (or applicable state wiretap laws for other Class Members);

E. For an order declaring that Defendants' acts and practices constitute common law invasion of privacy (intrusion upon seclusion);

F. Awarding Plaintiff and the Class Members restitution and disgorgement of all profits unjustly obtained by Defendants as a result of their unlawful conduct;

G. Awarding Plaintiff and the Class Members actual, statutory, and nominal damages in an amount to be proven at trial, including but not limited to damages available under 18 U.S.C. § 2520 and Tex. Civ. Prac. & Rem. Code § 123.004;

H. Awarding Plaintiff and the Class Members punitive damages in an amount sufficient to deter Defendants and others from similar conduct in the future;

I. Awarding Plaintiff and Class Members their reasonable attorneys' fees and litigation costs, to the extent permitted by law;

J. Granting such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: May 14, 2025

Respectfully submitted,

Reinaldo Aguiar, *Pro se*

2302 Britton Ridge Drive

Katy, TX 77494

TEL: (646) 299-5724

EMAIL: aguiar@reinaldo.ca

EXHIBIT A

May 14, 2025

AFFIDAVIT OF REINALDO AGUIAR

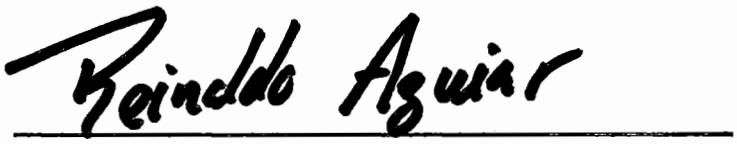
I, Reinaldo Aguiar, residing at 2302 Britton Ridge Drive, Katy, TX 77494, being duly sworn, depose and state that the following is true and correct to the best of my knowledge, information, and belief:

1. I am the Plaintiff in the above-captioned action and make this affidavit based on my personal knowledge.
2. On or around January 27, 2025, I conducted and recorded a Technical Demonstration outlining certain systems and data I discovered, which are relevant to the allegations in my Complaint.
3. The ideas, technical analyses, and observations presented in that Technical Demonstration, its recording, and any associated transcripts are accurate and correct to the best of my current abilities and form part of the basis for the allegations made in my Complaint.
4. The original recording of the Technical Demonstration can be downloaded at the following web address: https://storage.googleapis.com/reinaldo-aguiar/A
5. The original recording has also been made available on YouTube at: https://www.youtube.com/embed/E8dQy2qdYXE

5. The transcript of the Technical Demo can be downloaded at the following web address: https://storage.googleapis.com/reinaldo-aguiar/transcript.txt

Further Affiant sayeth naught.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.
Executed on May 14, 2025.



Reinaldo Aguiar

Plaintiff